IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA v. ROBERT BOWERS	Criminal No. 18-292

UNITED STATES' RESPONSE IN OPPOSITION TO DEFENSE MOTION TO SUPPRESS EVIDENCE FROM SOCIAL MEDIA ACCOUNT (MOTION TO SUPPRESS NO. 5)

AND NOW comes the United States of America, by its attorneys, Scott W. Brady, United States Attorney for the Western District of Pennsylvania, Troy Rivetti and Soo C. Song, Assistant United States Attorneys for said district, and Julia Gegenheimer, Special Litigation Counsel, Civil Rights Division, and hereby files its response in opposition to the defendant's motion to suppress evidence from a social media account, [redacted], (Motion to Suppress No. 5) (Doc. No. 292).

I. SUMMARY

Defendant Bowers makes two arguments in support of his motion: (1) that there existed a reasonable expectation of privacy in the non-public account[1] information disclosed by [redacted]; and (2) that although non-public information was provided unprompted by [redacted] to the United States prior to obtaining a search warrant, the court should suppress evidence obtained through a subsequent, valid search warrant. Significantly, in his challenge to the evidence seized from the defendant's [redacted] account, the defendant does not raise any arguments about the form or content of the search warrant itself.

[1] Defendant Bowers erroneously refers to the [redacted] account as a "private" account. In fact, posts and communications were accessible by the public.

The law is clear that because [redacted] provided information voluntarily there was no search, no Fourth Amendment violation, and suppression is utterly unwarranted. Even if there was some impropriety in the provision of account information by a private party, the United States, in an abundance of caution, sought a valid search warrant to re-acquire evidence based upon probable cause exclusive of the information voluntarily provided by [redacted]. Doc. No. 292, Exh. A. The search warrant functionally cured any speculative taint.

As a threshold matter, the defendant fails to establish standing to challenge the search of the [redacted] account and cannot assert a reasonable expectation of privacy in the non-public account information that he voluntarily provided to a third party, [redacted]. In its terms of use, [redacted] Doc. No. 292, Exh. A at 7.

Federal agents executed the search warrant upon the defendant's [redacted] account in good faith and would have inevitably discovered relevant non-public information through other independent means.

I. RELEVANT FACTUAL AND PROCEDURAL BACKGROUND

On October 27, 2018, the defendant, Robert Bowers, drove to the Tree of Life Synagogue and entered the building carrying multiple firearms, including a high-powered AR-15 rifle. The defendant opened fire, killing 11 congregants and injuring additional members of the Tree of Life, Dor Hadash and New Light congregations. While inside the Tree of Life Synagogue, the defendant made statements indicating his desire to "kill Jews." Law enforcement responded to the scene and the defendant also opened fire upon them, injuring four public safety officers. Doc. No. 10 at 1.

As alleged in the 63-count Superseding Indictment, prior to October 27, 2018, the defendant, using his public account on the website Gab.com, posted his belief that "jews are the children of satan;" authored several other posts that referred to Jewish people using anti-Semitic slurs; and demonstrated deep animosity toward those of the Jewish faith, extolling violence and death. See Doc. No. 44 at 1. On or about October 10, 2018, also on Gab.com, Bowers posted a criticism of the Hebrew Immigrant Aid Society (HIAS) and a link to a HIAS webpage listing Jewish congregations that were hosting refugee-related events. That list of congregations included the Dor Hadash Jewish congregation of Pittsburgh. In the posting, Bowers wrote, "Why hello there HIAS! You like to bring in hostile invaders to dwell among us? We appreciate the list of friends you have provided[.]" On the morning of October 27, 2018, just prior to entering the Synagogue, Bowers again publicly posted on Gab.com: "HIAS likes to bring invaders in that kill our people. I can't sit by and watch my people get slaughtered. Screw your optics, I'm going in." Doc. No. 44 at 2.

[redacted]e [redacted] See Gov. Exh. 1; see also Biesecker, Kunzelman, Balsamo, Suspect in synagogue slaying spewed online hate for Jews, Associated Press (Oct. 27, 2018), https://apnews.com/b1c50ba4f0964df89a266e490aea6961 ("In

a statement, Gab.com said it suspended the alleged gunman's account Saturday morning shortly after his name was mentioned on police radio chatter. The company said it backed up the content of the account and notified the FBI.").

[redacted] the Electronic Communications Privacy Act ("ECPA") which pertains to account records and contents stored by internet service providers, 18 U.S.C. §§ 2701-12, and allows for and protects emergency disclosures to law enforcement in circumstances involving death or serious bodily injury. 18 U.S.C. § 2702(b)(8) and (c)(4). [redacted]

Notwithstanding the voluntary provision of Bowers's account information [redacted] on October 28, 2018, the United States sought a search warrant for the [redacted] account. In the affidavit of probable cause, the government was forthcoming about what had transpired with [redacted]:

[redacted]

[redacted]

Doc. No. 292, Exh. A at 6-7.

The affidavit [redacted]

[redacted]

Id., Exh. A at 7.

The affidavit of probable cause submitted in support of the search warrant [redacted]

[redacted]

[redacted].[2] Id., Exh. A at 4-7.

Almost simultaneously with the reporting of Bowers's attack at the Tree of Life Synagogue, the media began publicly reporting upon comments and posts of the defendant's [redacted] outward-facing account and reproducing content and images of the same. [redacted]

[redacted] Images and posts of Bowers's communications were reproduced in the media. See Phillips, Bagavathi, Reid, Valasik, and Krishnan, Washington Post, (The daily use of Gab is climbing. Which talker might become as violent as the Pittsburgh

[2] The defendant, confusingly, makes repeated reference to the fact that some information provided voluntarily to the United States was used in a separate search warrant affidavit [redacted] Doc. No. 292, Exh. B. No such reference was included in the affidavit here and so consideration of probable cause at [redacted] is of no moment.

synagogue gunman? (Nov. 29, 2018) (researchers explain that they have a data set of all Gab.com posts since 2016, including all of Robert Bowers's posts);[3] Amend, Analyzing a terrorist's social media manifesto: the Pittsburgh synagogue shooter's posts on Gab, Southern Poverty Law Center, (Oct. 28, 2018) ("While Bowers' Gab account was deactivated by the company, a screen capture of it suggests he was extremely active on the network.").[4] The content and timing of the post that the defendant made just before entering the Synagogue was readily, publicly observed and reproduced. See Perez, Murphy, Marquez, Stapleton, and Hilk, On social media, suspect had posted "I'm going in" and frequently targeted Jews, CNN, (Oct. 27, 2018, 2:36 p.m.).[5]

III. LEGAL STANDARD AND ANALYSIS

A. No Search or Seizure

Defendant Bowers conspicuously ignores the valid search warrant that was properly obtained by the United States for all material in his [redacted] account. Instead, he advocates for suppression based on private action that was not governmental in nature and therefore outside the scope of the Fourth Amendment. [redacted]

Further, ECPA, which governs account records and contents stored by service providers [redacted] anticipates and protects online service providers who disclose information to law enforcement about users who use the service in the commission of a crime, or in response to an emergency involving death or serious bodily injury. 18 U.S.C. § 2702(b)(8) and (c)(4).

[3] https://www.washingtonpost.com/news/monkey-cage/wp/2018/11/29/the-daily-use-of-gab-is-climbing-which-talker-might-become-as-violent-as-the-pittsburghsynagogue-gunman/

[4] https://www.splcenter.org/hatewatch/2018/10/28/analyzing-terrorists-social-media-manifesto-pittsburgh-synagogue-shooters-posts-gab

[5] https://www.cnn.com/us/live/news/Pittsburghsynagogueshooting/h_bfaba765e6942d3b918 78c30ba4d8bd4

Before reaching the issue of whether unlawful warrantless police conduct occurred, "the preliminary question is whether a Fourth Amendment search has taken place at all. The Constitution does not apply to searches, reasonable or otherwise, by private individuals …" United States v. Miller, 152 F.3d 813, 815 (8th Cir. 1998). "Private searches are not subject to constitutional restrictions." United States v. Hall, 142 F.3d 988, 993 (7th Cir. 1998) (finding Fourth Amendment inapplicable to search of defendant's computer by private computer shop technician). The Fourth Amendment "is wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.'" United States v. Jacobsen, 466 U.S. 109, 113 (1984)[6] (citing Walter v. United States, 447 U.S. 649, 662 (1980) (Blackmun, J., dissenting)). The Supreme Court "has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." United States v. Miller, 425 U.S. 435, 443 (1976); Hoffa v. United States, 385 U.S. 293, 302, (1966) ("Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."); Jacobsen, 466 U.S. at 117-18.

[6] Under facts not present here, the Supreme Court has assessed whether the government's review of evidence exceeded the scope of the private search. For example, in United States v. Jacobsen, the Supreme Court upheld the examination and field test of white powder by federal agents of a package that had already been opened by a private freight carrier, 466 U.S. at 126 ("federal agents did not infringe any constitutionally protected privacy interest that had not already been frustrated as a result of private conduct. To the extent that a protected possessory interest was infringed, the infringement was de minimis and constitutionally reasonable."). See also Miller, 152 F.3d at 816. [redacted]

An agent's mere viewing what private parties freely make available for inspection does not violate the Fourth Amendment. See Coolidge v. New Hampshire, 403 U.S. 443, 487-490 (1971); Burdeau v. McDowell, 256 U.S. 465, 475-76 (1921); Jacobsen, 466 U.S. at 119-20 (where agent's inspection of contents of plastic bags revealed nothing more than the private search, "[i]t infringed no legitimate expectation of privacy and hence was not a 'search' within the meaning of the Fourth Amendment."). "[E]vidence secured by private searches, even if illegal, need not be excluded from a criminal trial." United States v. Ellyson, 326 F.3d 522, 527 (4th Cir. 2003) (quoted in United States v. Richardson,[7] 607 F.3d 357, 364 (4th Cir. 2010)). So too can the government permissibly use information provided to a government informant, despite a defendant's expectation that his associates would not disclose confidential information to authorities. United States v. White, 401 U.S. 745, 751-52 (1971).

As to [redacted] account, no legally cognizable search by the government occurred until a valid warrant supported by ample probable cause was authorized by a federal magistrate judge on October 28, 2018. The defendant has raised no challenge to the search warrant itself. Doc. No. 292, Exh. A. [redacted] Under ECPA, [redacted] had a safe-harbor under the statute to disclose information in response to an emergency involving death or serious bodily injury, conditions which were present in abundance here. See 18 U.S.C. § 2702(b)(8) and (c)(4).

[7] The facts of Richardson are analogous. The defendant in Richardson sought to suppress the results of the warrantless scan of his email account by his service provider, AOL, that resulted in the discovery of child pornography. AOL submitted that information to the National Center for Missing and Exploited Children. 607 F.3d at 361. The Fourth Circuit readily concluded that AOL's "actions did not equate to governmental conduct triggering constitutional protection." 607 F.3d at 364.

Although Supreme Court jurisprudence would have supported the review and use of that privately-provided information by the FBI, in this case, the United States, in an abundance of caution, opted to seek a search warrant supported by probable cause, [redacted]. Accordingly, there is no basis to suppress [redacted].

B. No Reasonable Expectation of Privacy

Defendant Bowers concedes that he cannot reasonably assert a subjective expectation of privacy in the public postings on the [redacted] account. Doc. No. 292 at 3. Instead, he alleges an impersonal, abstract interest in the non-public information that he voluntarily provided [redacted]. In support of his argument, Bowers inaptly invokes Carpenter v. United States and Riley v. California, attempting to draw parallels between cell site location information, cell phone contents, and the non-public information disclosed [redacted]. Any assertion of a privacy expectation by Bowers is without legal and factual support and, more importantly, is of no consequence because the ultimate search and seizure of [redacted] by the FBI was not warrantless.

1. Third Party Doctrine

The Supreme Court has "uniformly ... held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action." Smith v. Maryland,[8] 442 U.S. 735, 740 (1979) (collecting cases). For an "intrusion into [the] private sphere" to constitute a "search," a defendant must "seek[] to preserve something as private" and "society [must be] prepared to recognize [that privacy expectation] as reasonable." Carpenter v.

[8] In Smith, the Supreme Court rejected the defendant's argument that he had a "reasonable expectation of privacy" in the numbers that he dialed on his home telephone and held that Smith's expectation of privacy was "not one that society is prepared to recognize as reasonable" because he voluntarily turned the information over to a third party, the telephone company. Id. at 743–44 (citing Katz v. United States, 389 U.S. 347, 361 (1967)).

United States, 138 S. Ct. 2206, 2213 (2018) (quoting Smith, 442 U.S. at 740). Information shared with third parties is generally not protected by the Fourth Amendment pursuant to the third party doctrine. See Smith, 442 U.S. at 743-44 (the Supreme Court has "consistently … held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties"); United States v. Cox, 2020 WL 2899685, at *1 (N.D. Ind. June 3, 2020). The "third-party doctrine" is an exception to the Fourth Amendment warrant requirement that has its roots in Katz v. United States where the Supreme Court asserted that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection," 389 U.S. 347, 351 (1967). See Miller, 425 U.S. at 443 (no Fourth Amendment violation when information revealed to third party is later conveyed to government).

Generally, courts have not recognized a privacy interest as objectively reasonable where individuals are forewarned of a diminished privacy interest before engaging in an activity. See e.g., United States v. Young, 350 F.3d 1302, 1308 (11th Cir. 2003) ("No reasonable person would expect to retain his or her privacy interest in a packaged shipment after signing an airbill containing an explicit, written warning that the carrier is authorized to act in direct contravention to that interest"); Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) (online bulletin board's "disclaimer stating that personal communications were not private … defeats claims to an objectively reasonable expectation of privacy [by bulletin board] users"); United States v. Simons, 206 F.3d 392, 398 (4th Cir.2000) (finding no privacy interest in an employee's internet search records when an employer posted a privacy disclaimer regarding computer files).

Under the Fourth Amendment, Bowers's assertion of an expectation of privacy in the non-public records associated with his account is not reasonable as he voluntarily and willingly provided that information to the third party, [redacted]. Such user data does not constitute the

"private papers" of the defendant, but rather are maintained as business records [redacted]. See Miller, 425 U.S. at 440. Further, the defendant and all [redacted] users were placed on notice that any of their information may be shared with law enforcement:

[redacted]

[redacted], any subjective expectation of privacy by Bowers was not reasonable nor one that society is prepared to recognize. In any event, suppression would not follow even if this Court were to find a reasonable, subjective privacy interest in the non-public records maintained [redacted] because the [redacted] account information was obtained by a valid warrant, so no warrantless search occurred.

2. Account Records Not Protected

Significantly, the defendant does not seek to suppress the more incriminating evidence from his [redacted] account – posts that evince an animosity towards Jewish people and that immediately preceded the defendant's rampage (" … Screw your optics, I'm going in"). Doc. No. 292, Exh. A at 6. "When a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment." United States v. Meregildo, 883 F. Supp.2d 523, 525 (S.D. NY 2012) (citing Katz, 389 U.S. at 351). Because the defendant concedes that his public posts are not protected by the Fourth Amendment, in the context of his motion to suppress, it is instructive to consider what non-public records were associated with the [redacted] account. For reasons that are unclear, the defendant cites only to the text of a different search

[9] [redacted]; Doc. No. 292 Exh. A at 7.

warrant, Mag. No. 18-1398, that [redacted]. Doc. No. 292, Exh. C at 4.

Non-content [redacted] records include information like subscriber and IP information. They are administrative in nature, do not implicate privacy interests, are maintained by a third party, and could have been obtained with grand jury subpoenas or other process that did not require probable cause.

There is generally no privacy interest in records associated with electronic accounts held by third parties. Accordingly, the Fourth Amendment does not protect subscribers from the production of subscriber records by third-party service providers. United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008) (surveying cases); [10] United States v. Christie, 624 F.3d 558, 573-74 (3d Cir. 2010) (citing Perrine with approval for proposition that there is no reasonable privacy expectation in subscriber information and finding that defendant "had no reasonable expectation of privacy in his IP address and so cannot establish a Fourth Amendment violation"); United States v. Stanley, 2012 WL 5512987, at *12-17 (W.D. Pa., Nov. 14, 2012) (J. Conti) (acknowledging case law that no privacy interest exists in subscriber information and IP address records and finding that defendant had no "reasonable expectation of privacy in the signal which he voluntarily conveyed to a third party"), aff'd, 753 F.3d 114 (3d Cir. 2014); United States v. Morel, 922 F.3d 1, 9 (1st Cir. 2019), cert. denied, 140 S. Ct. 283 (2019) (no privacy interest in IP address information); see also In re Nickelodeon Consumer Privacy Litig., No. 12–cv–07829, 2014

[10] See Perrine, 513 F.3d at 1204 ("Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation") (citing Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001); United States v. Hambrick, 225 F.3d 656 (4th Cir. 2000) (unpublished), affirming United States v. Hambrick, 55 F. Supp. 2d 504, 508–09 (W.D. Va. 1999); United States v. D'Andrea, 497 F. Supp .2d 117, 120 (D. Mass. 2007); Freedman v. America Online, Inc., 412 F.Supp.2d 174, 181 (D. Conn. 2005); United States v. Sherr, 400 F. Supp. 2d 843, 848 (D. Md. 2005); United States v. Cox, 190 F. Supp. 2d 330, 332 (N.D.N.Y. 2002); United States v. Kennedy, 81 F.Supp.2d 1103, 1110 (D. Kan. 2000) and referencing Forrester, 512 F.3d at 510 (9th Cir. 2008); United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004).

WL 3012873, at *15 (D.N.J. July 2, 2014) ("Indeed, in the analogous Fourth Amendment context, email and IP addresses can be collected without a warrant because they constitute addressing information and do not necessarily reveal any more about the underlying contents of communications than do phone numbers, which can be warrantlessly captured via pen registers.") (citation and internal quotation marks omitted); United States v. Forrester, 512 F.3d 500, 509–10 (9th Cir. 2008) (comparing IP addresses to the outside of a letter and the monitoring of IP addresses to a pen register) (cited in United States v. Werdene, 188 F. Supp. 3d 431, 444 (E.D. Pa. 2016)).

It follows that the non-content, non-public records associated with the defendant's [redacted] account were not subject to a reasonable expectation of privacy, as they were generated by the defendant's voluntary, active use of [redacted] and constituted third party records outside of constitutional protection.

C. Defendant Lacks Standing

Aside from the many flaws in the defendant's challenge to the [redacted] evidence, Bowers also fails to establish his standing to seek suppression of that evidence in the first place. While the United States has set forth facts that demonstrate the defendant's connection to the [redacted] account, Bowers himself has failed to assert any personal privacy interest in the [redacted] records that he seeks to suppress, has failed to allege a single fact that indicates a possessory interest in the account, and phrases his arguments for suppression in the abstract.

The Fourth Amendment "protects people, not places." Katz, 389 U.S. at 351. A defendant may invoke the exclusionary rule "only if [he] demonstrates that his Fourth Amendment rights were violated by the challenged search or seizure." United States v. Padilla, 508 U.S. 77, 81 (1993) (citation omitted) (emphasis in original). It is the defendant's burden to establish that he had a reasonable expectation of privacy in the property searched and the item seized. Minnesota v.

Olson, 495 U.S. 91, 95–97 (1990); Rakas v. Illinois, 439 U.S. 128, 130 n.1 (1978); United States v. Stearn, 597 F.3d 540, 553 (3d Cir. 2010) (lower court "erred in ordering the suppression of evidence without regard to the defendants' ability to demonstrate legitimate expectations of privacy in the locations searched"). This requires the defendant to demonstrate both that he had a "subjective expectation of privacy in the area searched and that his expectation was objectively reasonable." United States v. Burnett, 773 F.3d 122, 131 (3d Cir. 2014).

A defendant may not simply rely on the government's intention to link a defendant to the accounts. See e.g., United States v. Watson, 404 F.3d 163, 166–67 (2d Cir. 2005); cf. United States v. Woodley, 2014 WL 3590143, at *4-5 (W.D. Pa. July 21, 2014) (J. Diamond) (defendant failed to establish reasonable expectation of privacy in cell phone records, including data location transmitted by the phone, where defendant proffered no evidence connecting him to the phone as its owner, subscriber, or authorized user); United States v. Hanner, 2007 WL 1437436, at *3-5 (W.D. Pa. May 14, 2007) (J. McVerry) (where defendant fails to establish legitimate expectation of privacy in a phone, he is foreclosed from asserting a challenge that the search of the phone was illegally executed)). Because the defendant has not met the threshold for standing, the Court should deny the motion to suppress.

D. Exclusionary Rule Does Not Apply – Good Faith Does Apply

On these facts, the extraordinary remedy of suppression sought by defendant Bowers is not appropriate even if this Court were to find some legally cognizable fault in the voluntary provision of account records [redacted]. Exclusion of the non-public [redacted] account information would serve no meaningful, deterrent effect because the United States did nothing to compel or persuade [redacted] to provide records prior to the issuance of a warrant.

"Whether to suppress evidence under the exclusionary rule is a separate question from whether the Government has violated an individual's Fourth Amendment rights." United States v. Katzin, 769 F.3d 163, 170 (3d Cir. 2014) (citing Hudson v. Michigan, 547 U.S. 586, 591-92 (2006)). A defendant thus has no constitutional right to suppression, and it "is not an automatic consequence of a Fourth Amendment violation." Herring v. United States, 555 U.S. 135, 137 (2009).

Courts have long recognized that the exclusionary rule imposes "substantial social costs" by hiding often crucial evidence and hindering the courts' truth-seeking function. United States v. Leon, 468 U.S. 897, 907 (1984). As a result, they have repeatedly affirmed that suppression "has always been our last resort, not our first impulse." Hudson, 547 U.S. at 591; Herring, 555 U.S. at 140; Katzin, 769 F.3d at 170. The police conduct at issue "must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." Herring, 555 U.S. at 144 (The exclusionary rule is meant only "to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence."). Where there is "an objectively reasonable good-faith belief that [the conduct] is lawful, or when [the] conduct involves only simple, isolated negligence, the deterrence rationale loses much of its force, and exclusion cannot pay its way." United States v. Franz, 772 F.3d 134, 145 (3d Cir. 2014) (quoting Davis v. United States, 564 U.S. 229, 238 (2011), and citing Herring, 555 U.S. at 137, Leon, 468 U.S. at 919, Katzin, 769 F.3d at 171).

Application of the exclusionary rule requires a careful balancing of suppression's significant costs against the possible value of deterrence. Relying on Supreme Court precedent, the Third Circuit has demanded a case-by-case cost-benefit analysis, rather than a categorical approach, when evaluating whether officers acted with objectively reasonable good-faith belief in

their actions. Franz, 772 F.3d at 145. This "fact-specific analysis is required," and "the need to weigh the costs and benefits of exclusion is constant." Id. at 146. Using this approach, the Third Circuit has declined to categorically exclude evidence, even where officers relied on warrants that were facially deficient. See, e.g., Franz, 772 F.3d 134; United States v. Wright, 777 F.3d 635 (3d Cir. 2015). The Circuit instead affirmed the need to examine the totality of the circumstances, such as the officer's conduct and knowledge, noting that the Supreme Court has "suggested that the absence of culpability is dispositive." Franz, 772 F.3d at 147, citing Davis, 564 U.S. at 238.

In this case, no governmental action prompted the voluntary provision of records by a private party. [redacted]. Out of an abundance of caution, the following day, the government obtained a valid search warrant to re-acquire the [redacted] account information. That warrant, which remains unchallenged by this defendant, did not rely upon the voluntarily-provided [redacted] data. Suppression would thus secure no benefit here. It would instead inflict the significant cost of excluding highly probative evidence that is plainly within the scope of the warrant and supporting affidavit, which remains unchallenged by the defendant, and that the government could have obtained in any case.

E. Independent Source, Inevitable Discovery

Assuming, arguendo, that the valid search warrant for the [redacted] account was tainted by the voluntary provision of [redacted] records [redacted], the defendant's motion to suppress must also be denied because the information would have been inevitably

discovered. The exclusionary rule does not apply when the prosecution has an independent, untainted source of the evidence or when the evidence would have been inevitably discovered. Murray v. United States, 487 U.S. 533, 537 (1988); Nix v. Williams, 467 U.S. 431, 443 (1984). Under the inevitable discovery doctrine, evidence obtained through a constitutional violation is still admissible if "the prosecution can establish by a preponderance of the evidence that the information ultimately or inevitably would have been discovered by lawful means." Nix, 467 U.S. at 444 (1984). "The independent source doctrine serves as an exception to the exclusionary rule and permits the introduction of 'evidence initially discovered during, or as a consequence of, an unlawful search, but later obtained independently from activities untainted by the initial illegality.'" United States v. Price, 558 F.3d 270, 281 (3d Cir. 2009) (quoting Murray, 487 U.S. at 537).

In United States v. Herrold, the Third Circuit analyzed the acquisition of child pornography files through an independent source, inquiring "(1) whether a neutral justice would have issued the search warrant even if not presented with information that had been obtained during an unlawful search and (2) whether the first [presumptively unlawful] search prompted the officers to obtain the [subsequent] search warrant." Herrold, 962 F.2d 1131, 1144 (3d Cir. 1992); see United States v. Stabile, 633 F.3d 219, 242-45 (3d Cir. 2011); Price, 558 F.3d at 282. "If the answers to these questions are yes and no respectively ... then the evidence seized during the warranted search, even if already discovered in the original entry, is admissible." Herrold, 962 F.2d at 1144. The effect of an independent source is to "vitiate the taint of the presumed illegal search." Stabile, 633 F.3d at 245.

While similar to the independent source doctrine, under the inevitable discovery doctrine, "if the prosecution can establish by a preponderance of the evidence that the information ultimately

or inevitably would have been discovered by lawful means ... then the deterrence rationale has so little basis that the evidence should be received." United States v. Vasquez De Reyes, 149 F.3d 192, 195 (3d Cir. 1998) (quoting Nix, 467 U.S. at 444); Stabile at 245. The government can meet its burden by establishing "that the police, following routine procedures, would inevitably have uncovered the evidence." Vasquez De Reyes, 149 F.3d at 195.

Applying the Herrold independent source analysis to the instant case demonstrates that any speculative taint by the voluntary provision of [redacted] records was vitiated by the subsequent warrant. As to the first inquiry, a neutral justice would have – and did, in fact – issue the search warrant [redacted]. Second, the private search that may have occasioned the provision of [redacted] account records [redacted] Gov. Exh. 2. Clearly, prior to the provision of [redacted] records [redacted], [redacted]. In effect, [redacted], the United States prophylactically employed its own independent source procedure by re-acquiring the records via a valid search warrant.

As to the inevitable nature of discovery, because of the open and notorious nature of [redacted] activity, the contents of his account were preserved, saved, and disseminated by the media and private parties almost immediately after the defendant's synagogue attack. In addition, [redacted]

[redacted] would have provided multiple inevitable means to discover [redacted].[11]

F. Defendant Not Entitled to Hearing

Defendant Bowers has not satisfied the necessary threshold for an evidentiary hearing. As this district ruled in United States v. Solomon, a defendant is not entitled to an evidentiary hearing on a pretrial motion in a criminal case unless he meets his "burden of establishing that a hearing is necessary," and that he has "stated a colorable claim." Solomon, 2007 WL 927960, at *1 (W.D. Pa. March 26, 2007). In Solomon, the court correctly relied upon the principles set forth in United States v. Voigt, 89 F.3d 1050, 1067 (3d Cir. 1996), and denied several motions to suppress search warrants without holding a hearing, as the defendants had failed to satisfy their threshold burden. Id. at *1.

Courts of appeals have long and repeatedly held that "evidentiary hearings on motions to suppress are not granted as a matter of course" but are held "only when the allegations and moving papers are sufficiently definite, specific, non-conjectural and detailed enough to conclude that a substantial claim is presented and that there are disputed issues of material fact which will affect the outcome of the motion." United States v. Villegas, 388 F.3d 317, 324 (7th Cir. 2004) (citations and internal quotations omitted); accord Wright et al., 3A Federal Practice & Procedure: Criminal § 689 (4th Ed. 2020); 27 Moore's Federal Practice (2020) § 641.193[2] & n.1; see also United States v. Richardson, 764 F.2d 1514, 1527-28 (11th Cir. 1985); United States v. Harrelson, 705 F.2d 733, 737 (5th Cir. 1983); United States v. Culotta, 413 F.2d 1343, 1345 (2d Cir. 1969); Cohen v. United States, 378 F.2d 751, 761 (9th Cir. 1967).

This widely-accepted standard is justified by the need to avoid convening unnecessary evidentiary hearings that waste scarce judicial resources and misuse the hearing as a tool to

[11] [redacted]

preview the trial evidence. "Hearings on motions to suppress are not discovery proceedings." Harrelson, 705 F.2d at 738.

Here, the defendant does not challenge that a valid search warrant was served [redacted] and that the defendant's account records were produced in response to that warrant. No evidentiary hearing is necessary for this Court to resolve defendant Bowers's legal arguments over the search of his social media account.

IX. CONCLUSION

The defendant's social media account evidence was obtained with a valid search warrant that contained ample probable cause. The [redacted] provision of information and records by a private, third-party provider did not constitute a warrantless search. For the reasons herein stated, the United States opposes the defendant's motion to suppress evidence, Doc. No. 292, and requests that this Court deny the motion in its entirety.

Respectfully submitted,

SCOTT W. BRADY
United States Attorney

By: s/Troy Rivetti
TROY RIVETTI
Assistant U.S. Attorney
PA ID No. 56816

s/Soo C. Song
SOO C. SONG
Assistant U.S. Attorney
DC ID No. 457268

s/Julia Gegenheimer
JULIA GEGENHEIMER
Special Litigation Counsel
Civil Rights Division
NY ID No. 4949475